Access Control Management System (ACMS)

<u>Background</u>

CPS - Physical Security Solutions in partnership with ITS - Administrative Technical Solutions developed a new database to replace the 1999 Key Control System (KCS) which has reached the end of its serviceable life. The new database is known as ACMS and while initially ACMS will primarily replace the functions that KCS offered. This new system will allow Access Control to provide departments with direct access to some data such as departmental key holder details so that the department can conduct periodic key audits and identify potential areas needing risk mitigation due to lost and stolen keys.

It is important to understand that a person can only be associated with a single primary department and as such, will normally be the department which initially requests a key/card for the person. While a person may no longer be with the original department, they will continue to be associated with and on reports for, the original department until such time as the key/card/fob/token is returned or we receive confirmation of the new department.

To follow privacy best practices, we are asking all SFU Access Control signing authorities to be configured for Multi-Factor Authentication (MFA). All faculty and staff will be returned to enroll in MFA by May 2021 but you can get setup today. To learn more about MFA, please visit https://www.sfu.ca/itservices/info_security/multi-factor-authentication.html and when you are able, please visit https://www.sfu.ca/itservices/info_security/multi-factor-authentication/set-up-mfa.html to get set up with MFA.

Once you have installed MFA, email accessct@sfu.ca and request login details for ACMS.

After you have been granted access to ACMS, you will be able to access the system and pull key reports related to people in your department and you will also be able to see who has been issued a Burnaby fob. As the system cannot communicate with Honeywell or Lenel, requests related to reports for the electronic access control system will be manually extracted and provided by Access Control staff. Please note that the system will refer to cards and fobs as tokens as we may also be looking at future options such as Bluetooth access tokens, NFC and other features.
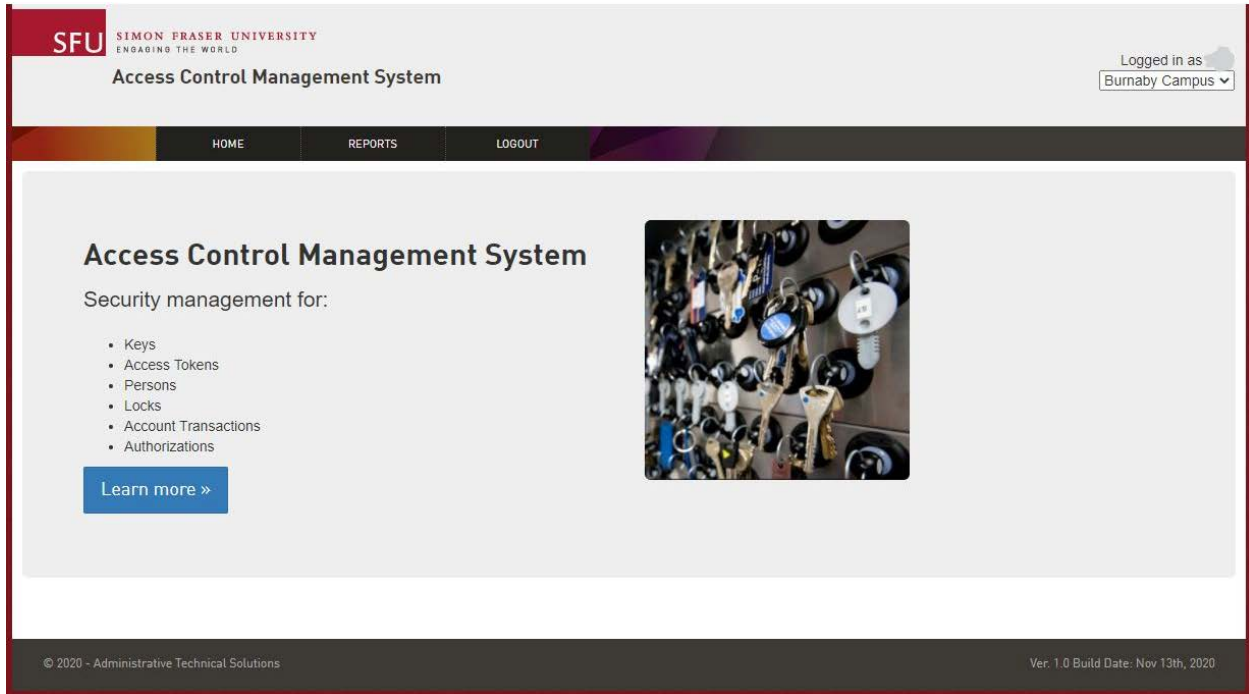
This is just the first version of the new system and we have lots of features we are evaluating for future versions including looking at options to phase out the existing MS Excel request form with an online request that will make selecting options much easier as the system (hopefully) be able to limit your options to what is valid for your department. We already have a long list of planned features to address once we finish migrating all the original KCS functions to ACMS but once things are stable we will look to our users for additional features that would provide value.

Please note that ACMS currently only contains data related to Burnaby key and fob holders.

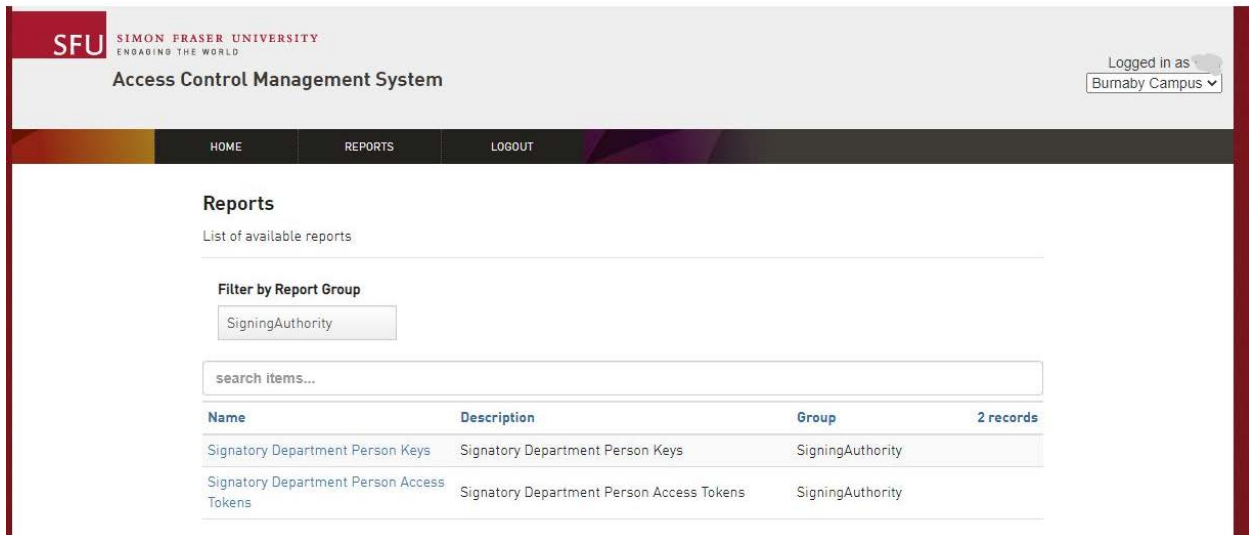The following pages provide a quick reference guide on how to use ACMS at this time.

USING ACMS AS A SIGNING AUTHORITY

When you first connect to ACMS you will be presented with the following screen (after authenticating):

Select reports from the top menu bar to see available reports:

When you select the key report you will need to select one or more departments (based on your permissions), a person's status and key status:

Tips & important information:

- It is recommended you select **all** person statuses but you may find it useful to limit the key status to issued for most audits (feel free to evaluate the options and output).
- Reports will export in .csv format (Comma Separated Value) that can be opened by MS Excel. The last two columns allow a department to confirm that the key is still held by the holder and any comments they need to share with access control.
  - NOTE: **Please do not remove any columns or modify other fields if you plan to use the report to have Access Control update records.**
- Keys marked as "conversion" generally are keys that no longer work as the lock was changed – these keys should be returned immediately. If a key is found to be marked as conversion but you know it still works, please provide all the details to accessct@sfu.ca ASAP so we can investigate and update our records.

We currently have a large number of keys that the holder or department have not confirmed the status, we are hoping you will be able to assist addressing any key that does not have an existing audit date. All types of master keys are considered higher risk and should be audited at least annually.

If you select the token report, you will be prompted a similar screen / options and the output will be similar:

NOTE:

- The token report does not directly communicate with either of our electronic access control databases (Honeywell / Lenel) as these systems are on segregated secure networks to protect from unauthorized access. You may request a Honeywell report for your department by emailing accessct@sfu.ca

Tip:

- Some departments have decided to use a common expiry date for all their staff cards such as the middle of July and a month prior they request a Honeywell report to confirm which fobs to renew for another year – as this can be done in bulk, it takes less time for everyone.